SUPPLEMENTAL REMARKS

Applicant has carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

Applicant thanks the Examiner for the courtesy of an interview granted to Applicant's representative David Zviel, registration number 41,392, on 14 September 2005. Examiner Christian Laforgia was also present at the interview. In the interview, the substance of which is described in the Interview Summary, a proposed amendment to claim 1 was discussed. Claim 1 has now been amended, as described below, substantially in accordance with the proposed amendment.

The abstract stands objected to. The abstract has been amended to overcome the objections.

The specification stands objected to because of use of the abbreviation "SIG" for "signature"; it is respectfully pointed out that the Office Action incorrectly identifies the abbreviation as an acronym. At the first use of "SIG" at line 16 of page 7, the specification states "assigning SIG as the signature of (M_X, M_Z), wherein SIG includes (x,y)". It is respectfully pointed out that the meaning and use of "SIG" are thus clearly indicated, so that persons skilled in the art would understand what "SIG" represents, and that therefore no correction of the specification is required.

Claims 1 - 15 stand rejected under 35 USC 101 as being directed to non-statutory subject matter. The Office Action correctly points out that the claims are directed towards a method for digitally signing a message, but rejects the claims on the grounds that the steps could theoretically be performed by a person using pen and paper. In the interview mentioned above, Applicant's representative suggested adding recitation that the method is performed in a computing device in order to overcome the rejection. However, it is respectfully pointed out that such an addition is unnecessary for the following reasons:

1. Originally filed claims 4 - 7 and 12 - 15 explicitly recite performing at least part of the method in a computation device; hence, the 35 USC 101 rejection of claims 4 - 7 and 12 - 15 is misplaced for that reason alone.

2. The recent opinion of the Board of Patent Appeals and Interferences in *ex parte Lundgren* (Appeal No. 2003-2088) confirms that the ground of rejection stated in the Office Action is not proper. The claims are directed to a useful process for digitally signing a message. The Office Action asserts that the steps could performed by a person using a pen and paper, but that is not determinative of whether the process is statutory subject matter. *See e.g. At&T Corp. v. Excel Communications, Inc.*, 172 F.3d 1352, 1358 (Fed. Cir. 1999). For the foregoing reasons, the applicant submits that the 35 USC §101 rejection of claims 1 - 15 should be withdrawn. Therefore, claim 1 has not been amended to recite that the method is performed in a computing device.

New claim 17, depending from claim 1 and reciting that the method is performed in a computing device, has been added. New claim 17 is supported, inter alia, by the fourth full paragraph on page 28 of the description.

Claims 1 - 16 stand rejected under 35 USC 112 as being indefinite. Amendments have been made to claim 1 to clarify the language thereof; the amendments are believed to overcome all of the rejections of claim 1 under 35 USC 112. The rejection of claim 1 under 35 USC 112 is therefore deemed to be overcome.

Claims 2 - 15 were rejected because of their dependency from claim 1; the rejection of claims 2 - 15 on this basis is therefore deemed to be overcome.

Claim 16 has been cancelled.

Claims 2, 3, 10, and 11 stand rejected because of lack of antecedent basis.

Claim 2 has been cancelled.

Claim 3 has been amended to correct the lack of antecedent basis; the amendment to claim 3 also corrects the lack of antecedent basis in claims 10 and 11.

Therefore, the rejection of claims 3, 10, and 11 under 35 USC 112 for lack of antecedent basis is deemed to be overcome.

Claims 11 - 15 stand rejected under 35 USC 112 for omitting essential steps. Claim 11 has been amended accordingly, and a consequent amendment has been made to claim 12; the amendment to claim 11 also overcomes the rejection of claims 12 - 15, which depend directly or indirectly from claim 11.

Therefore, the rejection of claims 11 - 15 under 35 USC 112 for omitting essential steps is deemed to be overcome.

Claim 16 stands rejected under 35 USC 112 for omitting essential structural cooperative relationships of elements.

Claim 16 has been cancelled.

Claims 1 - 3, 11, and 16 stand rejected under 35 USC 103(a) as being unpatentable over Ong et al ("An Efficient Signature Scheme Based on Quadratic Equations") in view of Okamoto et al ("An Efficient Digital Signature Scheme based on an Elliptical Curve over the Ring Z_N.")

Ong et al describes the OSS signature scheme.

Okamoto et al describes an elliptical curve signature scheme. Okamoto et al describes obfuscation by introduction of additional variables, but does not describe or suggest an improved OSS signature scheme; nor is it evident how Ong et al could be combined with Okamoto et al.

Claim 1 has been amended by adding additional recitation, supported, *inter alia*, by the specification on pages 11 and 12. The amendment to claim 1 makes the distinction of claim 1 over the prior art of record particularly clear.

Specifically in regards to the use in claim 1 of the relative word "close", Applicant notes that the term is used on page 12, lines 1 - 18 of the specification. Persons skilled in the art of cryptography will appreciate that "close", when referring to numbers in the context of cryptographic computations in modulo arithmetic, with the modulus n being a very large number, means that the two numbers would be considered "close" if they differ in size by only a small integer number of bits (that is, by only a few orders of magnitude base 2).

Claim 1 is therefore deemed allowable.

Claim 2 has been cancelled.

Claims 3 - 15 depend directly or indirectly from amended claim 1 and recite additional patentable subject matter. Claims 3 - 15 are therefore deemed allowable.

Claim 16 has been cancelled.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

9 November 2005

L. Friedman
Reg. No. 37,135

WELSH & KATZ, LTD.
120 South Riverside Plaza
22nd Floor
Chicago, Illinois 60606
(312) 655-1500